CLAIMS:

1. Apparatus for storage of data, comprising means for storing copies of a plurality of data items, means for generating at the end of a predetermined period of time, a data file comprising hash values of each data item created and/or stored during that time, means for generating a single hash value of said data file, and means for transmitting said single hash value to a remote location for storage and/or publication thereof (or of data representative thereof).

2. Apparatus according to claim 1, wherein said data file comprises a hash value of each of the data items created and/or stored during said predetermined period of time together with one or more of a file name, a path name, the file size and a time-stamp in relation to each data item.

3. Apparatus according to claim 1 or claim 2, wherein at said remote location, and second data file is created comprising said single hash value and one or more additional data items relating to said single hash value, and a single hash value, and a single hash value said second data file is created for storage and/or publication.

4. Apparatus for storage of data substantially as herein described with reference to the accompanying drawings.

5. A method of storing and authenticating data, comprising the steps of storing copies of a plurality of data items, generating at the end of a predetermined period of time, a data file comprising hash values of each data item created and/or signed during that time, generating a single hash value of said data file, and transmitting said single hash value to a remote location for storage and/or publication thereof (or of data representative thereof).

6. A method according to claim 5, including the steps of creating a second data file comprising said single hash value and one or more data items relating thereto, and creating a single hash value of said second data file for storage or publication..

7. A method according to claim 5 or claim 6, comprising the steps of retrieving a stored set of data items for a predetermined time period, generating a data file comprising the hash values of each of said data items, comparing one or more of said hash values with the corresponding hash value(s) contained in the data file generated in claim 5 to determine whether or not they match.

8. A method according to claim 7, further comprising the steps of generating a single hash value of the data file generated in claim 7, and comparing it with the corresponding single hash value generated in claim 1, to determine whether or not they match.

9. A method of storing and authenticating data substantially as herein described with reference to the accompanying drawings.

10. Apparatus for transmitting data between first and second end users via an information technology communications network, said first end user comprising means for encrypting a data item using a first identifier and transmitting said encrypted data item to said second end user module, said second end user comprising means for receiving said encrypted data item and transmitting an acknowledgement signal to said first end user, said first end user further comprising means for encrypting said first identifier using a second identifier and transmitting said encrypted first identifier to said second end user in response to receipt of said acknowledgement signal, said second end user further comprising means for requesting and receiving said second identifier in response to receipt of said encrypted first identifier, and means for decrypting said first identifier using said second identifier and for decrypting said data item using said first identifier.

11. Apparatus according to claim 10, wherein the second identifier is stored remotely from said first and second end users, preferably by a third party.

12. Apparatus according to claim 11, wherein said second identifier is transmitted to said remote storage location by said first end user in response to commencement of a data transfer transaction thereby.

13. Apparatus according to claim 12, wherein the transaction embodied by transmission of a second identifier to the remote storage location is time stamped.

14. Apparatus according to any one of claims 10 to 13, wherein a request for the second identifier to said remote storage location, the request being in the form of the encrypted data item or an encrypted version of the first identifier.

15. Apparatus according to any one of claims 10 to 14, wherein the data item is encrypted using a symmetric key and the first identifier or key is encrypted using an asymmetric key.

16. Apparatus according to any one of claims 10 to 15, wherein the acknowledgement signal may comprise an encrypted and/or compressed version, such as a hash value, of the original data item.

17. Apparatus for transmitting data between first and second end users, the apparatus being substantially as herein described with reference to the accompanying drawings.

18. A method for transmitting data between first and second end users via an information technology communications network, comprising the steps of encrypting by the first end user a data item using a first identifier and transmitting said encrypted data item to said second end user, receiving by said second end user said encrypted data item and transmitting an acknowledgement signal to said first end user, said first end user encrypting said first identifier using a second identifier and transmitting said

encrypted first identifier to said second end user in response to receipt of said acknowledgement signal, said second end user requesting and receiving said second identifier in response to receipt of said encrypted first identifier, decrypting said first identifier using said second identifier and decrypting said data item using said first identifier.

19. A method for transmitting data between first and second end users, the method being substantially as herein described with reference to the accompanying drawings.

20. Apparatus for verifying by a second end user the authenticity of use of an identifier by a first end user, the apparatus comprising means for identifying the communication of a data item encrypted using or otherwise including an identifier unique to said first end user from said first end user to said second end user across an information technology communications network, means for accessing, in response to such identification, storage means containing information relating to one or more valid recent events or transactions relating to said identifier which have occurred across said information technology communications network, means for obtaining confirmation from said first end user that at least one of said recent events or transactions is valid, and means for preventing further use of said identifier in the event that such confirmation is not received.

21. Apparatus for verifying by a second end user the authenticity of user of an identifier by a first end user, the apparatus being substantially as herein described with reference to the accompanying drawings.

22. A method for verifying by a second end user the authenticity of use of an identifier by a first end user, the method comprising the steps of identifying the communication of a data item encrypted using or otherwise including an identifier unique to said first end user from said first end user to said second end user across an information technology communications network, accessing, in response to such identification,

storage means containing information relating to one or more valid recent events or transactions relating to said identifier which have occurred across said information technology communications network, obtaining confirmation from said first end user that at least one of said recent events or transactions is valid, preventing further use of said identifier in the event that such confirmation is not received.

23. A method for verifying by a second end user the authenticity of use of an identifier by a first end user, the method being substantially as herein described with reference to the accompanying drawings.